Załącznik nr 2 do SIWZ

Szczegółowy opis przedmiotu zamówienia:

Dotyczy postępowania na: „Dostawę sprzętu komputerowego z oprogramowaniem”

1. Laptop……..130szt
   Kody CPV 30213100-6;
   30237410-6;
   30237220-7;
   48771000-3.

Laptop		
Zastosowanie		Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, przeglądania multimediów, dostępu do Internetu oraz poczty elektronicznej. Parametry techniczne komputera muszą zapewnić jego pełną funkcjonalność w w/w zakresie przez okres realizacji projektu tj. do 31.12.2015 roku, a następnie przez 5 letni okres trwałości projektu. Komputer zostanie użyczony jednostkom podległym objętym projektem.
Opis wymagań minimalnych		
1	Typ	Komputer przenośny
2	Wyświetlacz	Podświetlenie LED, min. rozdzielczość 1366 x 768, przekątna ekranu 15,6”
3	Procesor	Procesor uzyskujący wynik co najmniej 3500 punktów w teście Passmark - CPU Mark według wyników procesorów publikowanych na stronie http://www.cpubenchmark.net/cpu_list.php (w ofercie podać model i nazwę producenta procesora)
		Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testu Oferent musi dostarczyć Zamawiającemu licencjonowane oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.
4	Pamięć RAM	Min. 8 GB DDR3
		możliwość rozbudowy do min. 16 GB
		min. 1 wolne złącze dla rozszerzeń pamięci
5	Dysk twardy	min.500GB SATA
6	Napęd optyczny	Napęd DVD+/-RW DL SATA wewnętrzna wraz z oprogramowaniem do nagrywania płyt
7	Karta dźwiękowa	Zintegrowana
8	Karta sieciowa	Port sieci LAN 10/100/1000 Ethernet RJ 45 zintegrowany z płytą główną
		Karta sieciowa bezprzewodowa Wi-Fi 802.11 b/g/n, anteny wbudowane w obudowę
9	Karta graficzna	Zintegrowana min 128MB pamięci RAM wspierana technologią DirectX w wersji min 11

10	Czytnik kart	wbudowany min. SD
11	Porty	1x czytnik kart pamięci 1x wejście mikrofonowe/wyjście słuchawkowe (lub 1x wyjście słuchawkowe/audio oraz 1x wejście mikrofonowe) 3x USB (w tym co najmniej jeden port USB 3.0 lub 3.1) 1x RJ45 (sieciowy) 1x HDMI 1x D-Sub (wyjście na monitor) 1x DC - in (gniazdo zasilania)
12	Klawiatura	Pełnowymiarowa, z wydzieloną klawiaturą numeryczną obsługującą standard polski programisty.
13	Dodatkowe wyposażenie	Wbudowana/e: kamera, mikrofon, głośniki stereo.
14	Dodatkowe akcesoria	Torba dostosowana do wymiarów komputera, zasilacz, port Kensington Lock wraz z linką zabezpieczającą 1,5 m, mysz optyczna USB z rolką (scroll).
15	System operacyjny	patrz tabela system operacyjny
16	Bezpłatne oprogramowanie dodatkowe	Pakiet biurowy patrz tabela oprogramowanie biurowe
		Zainstalowane oprogramowanie do otwierania dokumentów w formacie PDF, program do obsługi archiwum (co najmniej formaty .zip, .rar, .7z), nagrywania płyt CD/DVD
17	Ergonomia pracy	Głośność przy maksymalnym obciążeniu nie może przekroczyć 40 dB
18	Bezpieczeństwo	Możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowym tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Funkcja ta ma wymuszać podanie hasła administratora przy próbie zmiany ustawień BIOS w sytuacji, gdy zostało podane hasło systemowe.
		Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.
		Naklejka antykradzieżowa, umieszczona w widocznym miejscu, o wymiarach 10cm x 6 cm z opisem „Zakup współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007 – 2013, projekt: **„Przeciwdziałanie wykluczeniu cyfrowemu w Gminie Miejskiej Starogard Gdański"",** po usunięciu naklejki zostanie trwały napis: „Własność Gminy Miejskiej Starogard Gdański, prośba o kontakt pod numerem telefonu 58 530 60 90 lub 58 530 61 07". Naklejka musi być wykonana zgodnie z wytycznymi zawartymi w Przewodniku w Zakresie Promocji Projektów Finansowanych w Ramach Programu Operacyjnego Innowacyjna Gospodarka 2007 – 2013 dla Beneficjentów i Instytucji Zaangażowanych we Wdrażanie Programu.
19	Gwarancja	Gwarancja min. 60 miesięcy door to door
		Wymagane okno czasowe dla zgłaszania usterek min. wszystkie dni robocze w godzinach od 8:00 do 16:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www, email lub telefoniczne.
		Musi być zapewniona możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

		Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.
20	Certyfikaty i normy	Certyfikat ISO9001 dla producenta sprzętu (załączyć do oferty).
		Certyfikat, potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym (załączyć wydruk ze strony producenta oprogramowania).
		Deklaracja zgodności CE (załączyć do oferty).
		Komputer musi spełniać wymogi normy Energy Star minimum 5.0. Wymagany wpis dotyczący oferowanego komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov – (Zamawiający wymaga przedłożenia wraz ofertą wydruku ze strony internetowej lub certyfikatu dla danego komputera).
		Uwaga: Zamawiający wymaga by do oferty dołączyć dokumenty potwierdzające spełnianie wyżej wymienionych warunków.
		Uwaga: Dopuszcza się by certyfikaty i wyniki testów były sporządzone w języku angielskim.

2. Listwa przeciwprzepięciowa……130szt
   Kod CPV 30236000-2

Listwa przeciwprzepięciowa		
1	Włącznik	Tak
2	Typ gniazda	Francuskie (typ E) lub Schuko (typ F)
3	Ilość gniazd	min. 5szt
4	Długość przewodu zasil.	min. 1,8m
5	Napięcie znamionowe	min. 230V AC
6	Prąd znamionowy	10A
7	Bezpiecznik prądowy	min. 1x10A/250V automatyczny
8	Zabezpieczenie przeciwprzepięciowe	Tak
9	Gwarancja	min. 60 miesięcy

3. System operacyjny……130szt
   Kod CPV 48771000-3

System operacyjny	
Opis wymagań minimalnych	
1	Zainstalowana wersja 64-bit systemu operacyjnego, zapewniająca poprawną obsługę aplikacji napisanych dla środowiska 32 bitowego - możliwością reinstalacji systemu do wersji 32-bit;
2	Zarówno system operacyjny jak i instalowane wraz z nim aplikacje powinny być w pełni spolszczone (menu systemu, komunikaty systemowe, pomoc kontekstowa);
3	Możliwość dokonywania darmowych aktualizacji (co najmniej przez okres trwania projektu, tzn. 5 lat) i instalowania poprawek systemu umieszczonych na witrynie internetowej producenta, w sposób automatyczny lub z możliwością wyboru instalowanych poprawek;
4	Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet, z witryny producenta systemu;
5	Witryna pozwalająca ściągać aktualizacje systemu operacyjnego i sterowników obsługiwana w języku polskim;
6	Poprawna obsługa protokołów IP w wersji v4 i v6;
7	Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
8	100% kompatybilność dostarczonego systemu z aplikacjami napisanymi dla środowiska Microsoft Windows XP, Vista, 7 (m.in. poprawna obsługa aplikacji napisanych dla środowisk .NET1.1, .NET2.0, .NET3.0, .NET4.0, aplikacji wymagających Direct X 11, Java Sun);
9	System musi mieć zainstalowane oprogramowanie do odtwarzania multimediów, przeglądania Internetu, klienta poczty elektronicznej. Ww. oprogramowanie powinno spełniać warunki z punktów 2 i 3
10	Wsparcie dla powszechnie używanych urządzeń peryferyjnych (urządzeń sieciowych, standardów USB, Plug & Play, Wi-Fi)

11	Interfejs użytkownika działający w trybie graficznym, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać;
12	Możliwość założenia wielu kont użytkowników, możliwość przypisania uprawnień do aplikacji/części systemu operacyjnego na poziomie użytkownika, możliwość założenia hasła użytkownika; możliwość eksportowania ustawień użytkownika do pliku i przenoszenia ich na inne, kompatybilne komputery
13	Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników
14	Zintegrowany z systemem moduł wyszukiwania informacji umieszczonych na dysku lokalnym
15	Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych
16	Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
17	Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji
18	Możliwość wdrażania polityk bezpieczeństwa – polityk dla systemu operacyjnego i dla wskazanych aplikacji
19	Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny
20	System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk
21	Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem
22	Wsparcie dla JScript i VBScript
23	Graficzne środowisko instalacji i konfiguracji;
24	Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
25	Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;
26	Udostępnianie modemu
27	Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej
28	Możliwość przywracania plików systemowych
29	Możliwość blokowania lub dopuszczania do użycia dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
30	100% zgodność z oferowanym sprzętem
31	Poprawna współpraca z istniejącymi w jednostkach domenami Active Directory w zakresie autentyfikacji i ustalania uprawnień użytkowników;
Oprogramowanie musi być zainstalowane na oferowanych komputerach oraz dostarczone wraz z nośnikami.	
Zamawiający informuje, że licencje praw najmu na system operacyjny (jeśli dotyczy) muszą umożliwiać użyczenie sprzętu osobo/podmiotom trzecim w celach niekomercyjnych oraz ewentualną zmianę podmiotu, na rzecz którego następować będzie użyczenie sprzętu komputerowego.	
Jednostki podległe Zamawiającemu, którym będzie użyczony sprzęt komputerowy będą wykorzystywać go przez okres trwania projektu, tj. do 31.12.2015 r., a następnie przez 5 letni okres trwałości projektu.	

4. Oprogramowanie biurowe……130szt
Kod CPV 48771000-3

Oprogramowanie biurowe		
Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:		
Opis wymagań minimalnych		
1	Pakiet zintegrowanych aplikacji biurowych musi zawierać:	a. edytor tekstów,
		b. arkusz kalkulacyjny,
		c. narzędzie do przygotowywania i prowadzenia prezentacji,
2	Edytor tekstów musi umożliwiać:	a. edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty
		b. wstawianie oraz formatowanie tabel
		c. wstawianie oraz formatowanie obiektów graficznych,
		d. wstawianie wykresów i tabel z arkusza kalkulacyjnego,
		e. automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
		f. automatyczne tworzenie spisów treści,
		g. formatowanie nagłówków i stopek stron,
		h. sprawdzanie pisowni w języku polskim
		i. określenie układu strony (pionowa/pozioma),
		j. wydruk dokumentów
		k. wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego
		l. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
3	Arkusz kalkulacyjny musi umożliwiać:	a. tworzenie raportów tabelarycznych,
		b. tworzenie wykresów liniowych, słupkowych, kołowych,
		c. tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
		d. wyszukiwanie i zamianę danych,
		e. wykonywanie analiz danych przy użyciu formatowania warunkowego,
		f. formatowanie czasu, daty i wartości finansowych z polskim formatem,
		g. zapis wielu arkuszy kalkulacyjnych w jednym pliku,
		h. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
4	Narzędzie do przygotowywania i prowadzenia	a. prezentowanie przy użyciu projektora multimedialnego,
		b. zapisywalne jako prezentacja do odczytu

	prezentacji musi umożliwiać przygotowywanie prezentacji multimedialnych, które będą:	c. umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
		d. umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, możliwość tworzenia animacji obiektów i całych slajdów
5	Licencja	Zamawiający wymaga Licencji Rental lub równoważnego dla oprogramowania biurowego, jeżeli jest wymagane dla prawidłowego przekazania oprogramowania w użyczenie i przekazanie na własność po okresie trwałości projektu dla jednostek podległych.
Pakiety biurowe muszą być zainstalowane na oferowanych komputerach oraz dostarczone wraz z nośnikami.		
Zamawiający informuje, że licencje na oprogramowanie biurowe (jeśli dotyczy) muszą być udzielone na czas nieoznaczony, w sposób nie naruszający praw osób trzecich oraz muszą umożliwiać Zamawiającemu bez dodatkowych kosztów użyczenie oprogramowania na dowolny okres jednostkom podległym oraz muszą umożliwiać ewentualną zmianę jednostki podległej, na rzecz której następować będzie użyczenie oprogramowania biurowego.		
Jednostki podległe Zamawiającemu, którym będzie użyczony sprzęt komputerowy będą wykorzystywać go przez okres trwania projektu, tj. do 31.12.2015 r., a następnie przez 5 letni okres trwałości projektu.		

5. Oprogramowanie zabezpieczające ……130 licencji
Kod CPV 48771000-3

Oprogramowanie zabezpieczające		
Opis wymagań minimalnych		
1	Ogólne	Użytkownik musi mieć możliwość wielokrotnej re-instalacji programu na każdym ze stanowisk komputerowych zawartych w licencji, w tym bezpłatnej migracji na najnowszą edycję programu lub wersję kompatybilną z dowolnym innym systemem operacyjnym wspieranym przez program
		Pomoc techniczna dla programu powinna być świadczona w języku polskim przez polskiego dystrybutora lub producenta programu przez cały okres trwania umowy.
		Wsparcie powinno obejmować wsparcie online (zdalnie), poprzez email oraz telefoniczne
		Przez cały okres trwania umowy zamawiający będzie miał dostęp do bezpłatnej aktualizacji baz sygnatur wirusów.
		Okres ochronny minimum 62 miesiące od dnia dostawy komputerów i ich odbioru ostatecznego.
		Nie jest wymagana możliwość instalacji lub reinstalacji programu po zakończeniu abonamentu obejmującego aktualizację baz wirusów.
2	Program antywirusowy dla systemów	Pełna obsługa systemów Windows XP SP3 /Vista SP 2 /Windows 7 SP1/ Windows 8/10/Server2003 SP2/Server2008 SP2/Server2008R2 SP1/Server2012
		Pełne wsparcie dla systemów 32 i 64 – bitowych.
		Wsparcie dla Centrum zabezpieczeń (Windows XP), Centrum akcji (Windows 7).
		Interfejs programu dostępny w wersji polskiej oraz angielskiej.
		Pomoc dostępna z poziomu programu w wersji polskiej i angielskiej.
		Dokumentacja programu dostępna w wersji polskiej i angielskiej.
		Ochrona wyposażona w bazę danych zawierającą następujące warianty szkodliwych obiektów: wirusy, robaki, trojany, exploity. Powinna zawierać mechanizmy heurystyczne.
		Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, backdoor oraz narzędzi hakerskich.
		Rezydentny skaner wszystkich otwieranych, zapisywanych i uruchamianych plików.
		Możliwość skanowania wybranych plików, katalogów, dysków w tym dysków przenośnych i sieciowych.
		Możliwość skanowania skompresowanych i spakowanych plików i katalogów.
		Możliwość skanowania wszystkich formatów plików.
		Możliwość wyłączenia ze skanowania określonych katalogów, plików i plików z określonymi rozszerzeniami.
		Możliwość uruchomienia skanera na żądanie.

		Możliwość definiowania wielu różnych zadań skanowania (np. co godzinę, po włączeniu komputera, przy zalogowaniu), każde zadanie może być uruchamiane z różnymi ustawieniami (priorytet, wybrane obiekty do skanowania, czynności po wykryciu zagrożenia).
		Funkcja szybkiego skanowania pozwalająca na skanowanie istotnych funkcji systemu bez konieczności skanowania całego dysku.
		Wbudowana lista plików – nosicieli, czyli rozszerzeń plików narażonych na infekcję.
		Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, bez konieczności zmian w konfiguracji klienta pocztowego oraz niezależnie od zainstalowanego na stacji roboczej klienta pocztowego.
		Możliwość określania różnych numerów portów POP3 na których ma odbywać się skanowanie poczty przychodzącej.
		Skanowanie ruchu odbywającego się przez protokół HTTP na stacji roboczej.
		Możliwość zdefiniowania różnych portów HTTP na których ma odbywać się skanowanie.
		Integracja skanera HTTP z dowolną przeglądarką internetową, bez konieczności zmiany jej konfiguracji.
		Skaner ma mieć możliwość skanowania z wykorzystaniem algorytmów heurystycznych na kilku poziomach
		Skaner ma posiadać automatyczną aktualizację modułów analizy heurystycznej.
		Możliwość automatycznego lub ręcznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta.
		Wysyłanie zagrożeń nowo odkrytych przez mechanizmy heurystyczne powinno być możliwe z serwera zdalnego zarządzania oraz z każdej lokalnej stacji roboczej na której zainstalowany jest program antywirusowy.
		Możliwość ręcznego wysłania próbki nowego zagrożenia (podejrzanych plików) wraz z komentarzem oraz adresem email użytkownika, na który producent może wysłać dodatkowe pytania dotyczące wykrytego zagrożenia.
		Dane statystyczne zbierane przez producenta powinny być całkowicie anonimowe.
		W przypadku wykrycia zagrożenia ma istnieć możliwość wysłania przez program powiadomienia na wybrane adresy email użytkownika.
		Program musi posiadać możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego, zaś w przypadku wykrycia braku wymaganych aktualizacji umożliwiać opcję informowania użytkownika np. za pomocą zestawienia brakujących aktualizacji.
		Program musi mieć: możliwość definiowania aktualizacji systemowych i informowania o ich braku, podział aktualizacji pod względem ich istotności, a także możliwość całkowitej dezaktywacji tego komponentu
		System antywirusowy musi umożliwiać użytkownikowi przygotowanie płyty CD/DVD z której będzie dokonywać uruchomienia komputera w przypadku infekcji.
		System antywirusowy uruchomiony z płyty musi pracować w trybie tekstowym i mieć możliwość aktualizacji baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
		Program musi być wyposażony w moduł zapory sieciowej (personal firewall).

		Moduł zapory sieciowej musi kontrolować cały ruch przychodzący i wychodzący.
		Powinna istnieć możliwość całkowitego wyłączenie modułu zapory sieciowej. Dezaktywacja powinna być możliwa przynajmniej na dwa sposoby : na stałe i do ponownego uruchomienia komputera.
		Zapora sieciowa programu powinna obsługiwać protokół IPv6.
		Moduł zapory sieciowej musi mieć możliwość wyboru trybu pracy, w tym przynajmniej : automatycznym, automatycznego uczenia się, ręcznym – opartym na regułach użytkownika.
		Moduł zapory sieciowej musi umożliwiać definiowanie listy zaufanych aplikacji.
		Moduł zapory sieciowej musi umożliwiać ręczne dodawanie reguł i wyjątków.
		Podczas tworzenia reguł zapory sieciowej powinna być możliwość określania przynajmniej : kierunku ruchu, portu i/lub zakresu portów, oraz adresu serwera dla programu w sieci lokalnej
		W trakcie tworzenia reguł zapory sieciowej powinna istnieć możliwość wyboru przynajmniej dwóch akcji : zezwól, zablokuj.
		Możliwość definiowania profili z różnymi zestawami reguł dla różnych sieci, w których pracuje komputer.
		Program antywirusowy musi być w wyposażony w możliwość zabezpieczenia zmian konfiguracji hasłem.
		Program musi być wyposażony w automatyczną, przyrostową aktualizację baz wirusów i innych zagrożeń. Aktualizacja powinna być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD, USB, lokalnego repozytorium.
		Program musi obsługiwać aktualizację przez serwer proxy.
		Program musi posiadać dziennik zdarzeń, rejestrujący informację o pracy programu, przeprowadzonych aktualizacjach i wykrytych zagrożeniach.
		Pogram musi umożliwiać blokadę nośników wymiennych, w tym dysków USB i pamięci przenośnych
		Program musi zawierać moduł pozwalający na ograniczanie swobody dostępu do Internetu wyznaczonym użytkownikom.
		Program musi zawierać mechanizm odpowiedzialny za wczesne wykrywanie i dezaktywację nowych zagrożeń, nie ujętych jeszcze w bazach szkodliwego oprogramowania.
		Program musi zawierać funkcjonalność pozwalającą na migrację produktu do nowszej wersji (bezpłatnie w ramach aktywnego abonamentu) bez potrzeby deinstalacji wersji poprzedniej.
3	Ochrona rodzicielska	Oprogramowanie zabezpieczające powinno być wyposażone w moduł ochrony rodzicielskiej.
		Moduł musi mieć co najmniej polski interfejs użytkownika i pomoc w programie.
		Możliwość blokowania wybranych stron internetowych.
		Działanie programu w tle w sposób niewidoczny dla użytkownika systemu.
		Dostęp do ustawień programu zablokowany hasłem.
4	Konsola zdalnej administracji	Program musi zawierać moduł pozwalający na centralne zarządzanie dostępem do Internetu na poszczególnych stacjach z poziomu konsoli administracyjnej

		Praca programu powinna być niezauważalna dla użytkownika.
		Pełna obsługa systemów Windows XP SP3 /Vista SP2 /Windows 7 SP1/ Windows 8/ Windows 8.1/ Windows 10/Server2003 SP2/Server2008 SP2/Server2008R2 SP1/Server2012
		Pełne wsparcie dla systemów 32 i 64 – bitowych.
		Do instalacji serwera centralnej administracji nie może być wymagana instalacja dodatkowego oprogramowania (w szczególności Internet Information Services czy Apache).
		Do instalacji serwera centralnej administracji nie jest wymagana instalacja dodatkowego oprogramowania dla baz danych
		Musi zawierać centralne zarządzanie programami służącymi do ochrony stacji roboczych Windows.
		Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych (pojedynczych lub należących do konkretnych grup) i przesłania raportu ze skanowania do konsoli administracyjnej.
		Możliwość sprawdzenia poziomu ochrony stacji roboczych (przynajmniej aktualnych ustawień programu, wersji programu, bazy wirusów, wyników skanowania).
		Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej (adresów IP, wersji systemu operacyjnego, uruchomionych procesów, zainstalowanych aplikacji).
		Możliwość skanowania sieci w celu wyszukania niezabezpieczonych stacji roboczych.
		Możliwość zbierania z pozycji administratora informacji o nieprawidłowościach w pracy pakietów zainstalowany na stacjach klienckich, w tym przynajmniej: o procencie stacji podłączonych do sieci nie posiadających zainstalowanej lub posiadających nieaktywną ochronę, o stacjach posiadających nieaktualną wersję programu lub nieaktualną bazę wirusów.
		Możliwość zdalnego restartu, wyłączenia wybranych stacji roboczych (pojedynczych lub należących do konkretnych grup).
		Możliwość zdalnego podglądu pulpitu wybranych stacji roboczych (pojedynczych lub należących do konkretnych grup).
		Możliwość zdalnego uruchomienia na wybranych stacjach roboczych aplikacji/polecenia na uprawnieniach zwykłego użytkownika lub z wysokimi uprawnieniami.
		Możliwość sprawdzania liczby stanowisk wykorzystywanych w ramach poszczególnej licencji będącej w posiadaniu użytkownika
		Możliwość zarządzania stacjami znajdującymi się poza domeną.
		Możliwość zdalnego zarządzania opcją blokady nośników
Oprogramowanie zabezpieczające musi być zainstalowane na oferowanych komputerach oraz dostarczone wraz z nośnikami. Licencje powinny zostać dopasowane do zapotrzebowania zamawiającego.		

6. Serwis ……130 stanowisk
Kod CPV 50300000-8

Serwis		
1	Warunki ogólne	Pierwsza instalacja sprzętu komputerowego oraz świadczenie przez okres realizacji projektu, tj. do 31.12.2015 roku, usługi serwisu, helpdesku, infolinii dla jednostek podległych (130 zestawów komputerowych zakupionych w projekcie).
2	Miejsce świadczenia usługi	Adresy jednostek podległych, dla których będzie świadczona zamawiana usługa zostały określone w pkt. 2.7 SIWZ.
3	Helpdesk i infolinia	Wykonawca ma za zadanie stworzenie jednolitego, pojedynczego punktu przyjmowania telefonicznych, faksowych i elektronicznych (e-mail) zgłoszeń awarii kierowanych przez jednostki podległe (JP) oraz Zamawiającego. Telefoniczne odbieranie zgłoszeń musi odbywać się poprzez personel przygotowany do świadczenia pomocy, także osobom niepełnosprawnym. Niedopuszczalne jest do tego celu używanie automatów zgłoszeniowych. Połączenie z konsultantem musi zostać nawiązane w ciągu 30 sekund od momentu wybrania numeru infolinii. Nie ma ograniczeń, co do ilości podejmowanych przez Wykonawcę zgłoszeń i świadczenia usługi helpdesku/serwisu w ciągu całego okresu świadczenia usługi. Przyjmowanie zgłoszeń odbywać się będzie minimum w godzinach od 9 do 17 (e-mail, telefon, faks) przez 5 dni w tygodniu od poniedziałku do piątku, przez cały okres trwania umowy.
4	Zakres usług helpdesk/ servicedesk	1) Przyjmowanie zgłoszeń o: a) awariach sprzętu komputerowego dostarczonego przez Wykonawcę, b) awariach sprzętu peryferyjnego dostarczonych przez Wykonawcę, c) kradzieży lub zagubieniu sprzętów. 2) Podejmowanie czynności serwisowych polegających na: a) zainstalowaniu sprzętu komputerowego w jednostkach podległych pod adresami wskazanymi przez Zamawiającego. b) wstępnym weryfikowaniu przyczyny awarii, na podstawie informacji dostarczonych przez JP, c) udzielaniu porad i wyjaśnień JP dotyczących sprzętów i oprogramowania dostarczonego przez Wykonawcę, w tym zdalną pomoc w samodzielnym przywróceniu przez JP stanu początkowego systemu operacyjnego z partycji Recovery, d) usuwaniu usterek i awarii sprzętu komputerowego, oprogramowania i urządzeń peryferyjnych, nie objętych serwisem gwarancyjnym, e) wyjazdach serwisowych do JP, związanych z usuwaniem usterek, f) przekazywaniu zgłoszeń o kradzieży i zaginięciu sprzętu do Zamawiającego,

		g) przekazywaniu informacji o awariach i koordynowaniu czynności gwarancyjnych pomiędzy uczestnikami projektu a podmiotem odpowiedzialnym za świadczenie gwarancji. 3) Usługa serwisowa, poza czynnościami wymienionymi powyżej polegać ma również na optymalizacji i konserwacji sprzętu oraz raportowaniu pracy, w tym: a) re-instalacji systemu i oprogramowania wyspecyfikowanego w załączniku nr 2 do SIWZ dla JP, na podstawie złożonego przez nich pisemnego/telefonicznie/elektronicznie/faksowo zgłoszenia, b) dokonywaniu dodatkowych instalacji oprogramowania na wniosek Zamawiającego, c) konsultacjach telefonicznych dla JP oraz przedstawicieli Zamawiającego, d) ewidencjonowaniu zgłoszeń awarii, konsultacji telefonicznych i ich statusów oraz udostępnianie tych informacji Zamawiającemu na bieżąco do wglądu za pośrednictwem strony www lub drogą e-mailową. Przy wyborze drogi e-mailowej zaktualizowana ewidencja powinna być przesyłana co najmniej raz w tygodniu, a także na wezwanie Zamawiającego na wskazany przez niego adres poczty elektronicznej. Ewidencja powinna umożliwiać filtrowanie listy zawartości.
5	Inne ustalenia	Po zakończeniu instalacji / naprawy Wykonawca jest zobowiązany do kontroli poprawności działania komputera, oprogramowania i/lub urządzenia peryferyjnego. Wszelkie koszty związane z naprawą, transportem i wymianą sprzętu ponosi Wykonawca. Wykonawca zobowiązany jest do naprawy powstałych błędów w funkcjonowaniu oprogramowania, w tym do ewentualnej re-instalacji oprogramowania. Zamawiający zastrzega, że przez opiekę serwisową rozumie się także wszelką inną obsługę techniczną wykraczającą poza obowiązki wynikające z gwarancji.
6	Terminy	Czas reakcji serwisanta na podjęcie czynności serwisowych dotyczących sprzętu wynosi 24h, liczonych od chwili przyjęcia zgłoszenia usterki. Czas usunięcia usterki wynosi 4 dni roboczych, liczonych od momentu przyjęcia zgłoszenia. Usunięcie usterki powinno odbywać się, jeśli to możliwe, w systemie *on-site.* W przypadku stwierdzenia nieprawidłowości wykonania zadań serwisowych Zamawiający ma prawo do reklamacji usługi i nieodpłatnego wykonania ponownego serwisu w ciągu 48 godzin od momentu zgłoszenia przez upoważnionego przedstawiciela Zamawiającego nieprawidłowości w wykonaniu usługi serwisu. Wykonawca zobowiązany jest w ostatnim tygodniu każdego roku kalendarzowego trwania umowy do wykonania i dostarczenia do Zamawiającego raportów rocznych o zgłoszonych przez jednostki podległe lub Zamawiającego awariach i usterkach oraz o przeprowadzonych naprawach i wymianach sprzętu. Okres związania umową kończy się 31.12.2015 r.